VCRI
THE VALUE CHAIN
RISK INSTITUTE

VCRI LEARN · POST-QUANTUM CRYPTOGRAPHY

Why quantum breaks RSA

Shor’s algorithm, worked by hand on the number 15, and why post-quantum crypto is different.

Joshua Marpet and Cairn Viktor

THE FOUNDATION

RSA rests on one hard direction

Your public key holds the product. Your private key depends on the two primes.

Easy: multiply

$$3 \times 5 = 15$$

Any computer multiplies two 300-digit primes in a blink.

Hard: un-multiply

$$15 = ? \times ?$$

Splitting a 600-digit product back into its primes is out of reach for classical computers.

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

STEP 1, THE IDEA

A remainder is just a clock



Picture a clock with 15 hours instead of 12, numbered 0 to 14.

Count 49 hours around it. You pass 15, 30 and 45, then land on 4.

That is all “49 mod 15 = 4” means: where you land on the clock.

valuechainrisk.org/learn · CC BY 4.0

STEP 1, THE WORK

Keep multiplying by 7 and see where you land

STEP	MULTIPLY	LANDS ON THE 15-HOUR CLOCK
Start		1
1	1 × 7 = 7	7
2	7 × 7 = 49	4 (49 = 45 + 4)
3	4 × 7 = 28	13 (28 = 15 + 13)
4	13 × 7 = 91	1 (91 = 90 + 1), back where we started

valuechainrisk.org/learn · CC BY 4.0

STEP 1, THE PICTURE

The hops make a loop. Its length is the rhythm.



1 → 7 → 4 → 13 → 1

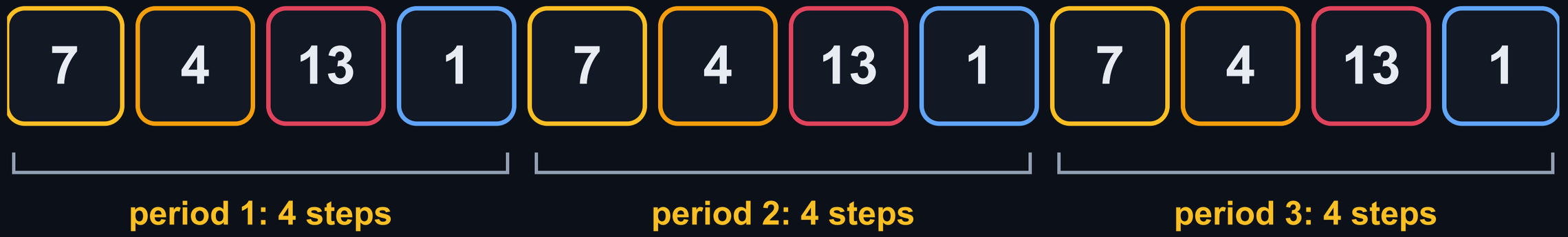
Four hops and you are home. Then the same four hops repeat, forever.

The period is r = 4. Finding that number is the whole game.

valuechainrisk.org/learn · CC BY 4.0

STEP 1, THE RHYTHM

Written out, it repeats like a drumbeat



A quantum computer is a machine for hearing exactly this kind of beat. Hold on to that; we come back to it.

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

STEP 2, WHY IT WORKS

Why a rhythm gives away the factors

A loop of 4 means

7^4 lands on 1, so $7^4 - 1$ is a multiple of 15.

$2400 = 15 \times 160$

Split it in half

$7^4 - 1 = (7^2 - 1) \times (7^2 + 1)$

$2400 = 48 \times 50$

15 must hide inside

15 divides 48×50 but neither number alone.

So 15's factors are split between them: 3 in 48, 5 in 50.

valuechainrisk.org/learn · CC BY 4.0

STEP 2

The rhythm cracks it

Step 2 is easy on any laptop. Step 1 is the wall: at real RSA size, the pattern runs for an astronomically long time before it repeats.

Half the period

r = 4, so use $7^2 = 49$. One below and one above: 48 and 50.

→

Shared factors

gcd(48, 15) = 3
gcd(50, 15) = 5

→

Cracked

3 × 5

valuechainrisk.org/learn · CC BY 4.0

THE QUANTUM STEP

What the quantum computer adds

Like hearing a note's pitch without counting every vibration. Elliptic-curve crypto hides the same kind of structure, so Shor breaks it too.

Classical computer

Walks the pattern step by step to see where it repeats.

At 2048 bits, no classical machine can finish the walk.

Quantum computer

Holds the whole pattern in superposition and hears its rhythm.

The quantum Fourier transform makes wrong answers cancel and the right period reinforce, like waves.

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

POST-QUANTUM

No rhythm to find

Noise is the defense: it erases the clean, periodic structure Shor needs.

Lattices

ML-KEM (from Kyber) and ML-DSA (from Dilithium), NIST FIPS 203 and 204.

A grid of points in hundreds of dimensions. You get a point nudged off the grid: which grid point is closest? Easy in 2D. In hundreds of dimensions, with deliberate noise, there is no known fast method, classical or quantum.

Hash-based signatures

SLH-DSA (from SPHINCS+), NIST FIPS 205.

Security rests only on hash functions being one-way. Almost no math structure to attack. Bigger signatures, very conservative design.

valuechainrisk.org/learn · CC BY 4.0

QUESTIONS EVERYONE ASKS

Two follow-ups

Is AES broken too?

No. Grover's algorithm roughly halves symmetric key strength.

AES-256 behaves like AES-128 against a quantum attacker, which is still considered strong.

Why care before the machines exist?

Harvest now, decrypt later: traffic recorded today can be read once the machines arrive.

Signatures add "forge later": long-lived signing keys and the things they vouch for.

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

WHAT TO DO MONDAY

Start with an inventory

- Find it: where do you use RSA and elliptic-curve keys? TLS, VPNs, SSH, code signing, document signing, device identity.
- Rank it: which data must stay secret, or which signatures must stay trustworthy, for ten years or more?
- Ask your vendors: what is your post-quantum plan, and when do you support ML-KEM?
- Prefer hybrid: classical plus post-quantum key exchange, so you are covered if either one fails.

valuechainrisk.org/learn · CC BY 4.0

VCRI

THE VALUE CHAIN
RISK INSTITUTE

Free to use, teach and share.

This deck is part of the VCRI Learn series. Use it in your class, your team meeting or your chapter, with credit to The Value Chain Risk Institute.

valuechainrisk.org/learn

valuechainrisk.org/learn · CC BY 4.0